PREVOTY

#1 GLOBAL PAYMENTS COMPANY OPTIMIZES SECURE DEVELOPMENT PROCESS WITH PREVOTY

Trusted payments provider with deeply embedded secure development culture partners with Prevoty for standardized, real-time application protection

June 2015

SUMMARY

The payments industry seems to adopt exciting new innovations every month (e.g. the Internet of Things, Bitcoin, mobile pay, Chip & PIN, biometrics, etc.), but its top application security threats have pretty much remained the same...for many years. Discover how a leading Global Payments Technology Company improved its secure software development life cycle (SSDLC) with a new runtime protection capability.

COMPANY BACKGROUND

This major Global Payments Technology Company's service-oriented portfolio includes over 2,000 applications that interact with hundreds of millions users, organizations and merchants worldwide. Their functions run the gamut – from financial transaction processing to payment enablement at point-of-sale terminals and gateways, rewards programs, web services, mobile applications, development platforms, APIs for external services, and more.

With such a large software mix handling extremely sensitive data and billions of transactions daily, any major service interruption or corruption can impact the world's markets, governments and socioeconomic infrastructures. It's no surprise that security and reliable performance dominate the company's list of priorities.

A FOCUS ON SECURE SOFTWARE DEVELOPMENT

The company's advanced information security leadership team understands that application security is uniquely challenging because it requires human intervention and thus introduces human error. Therefore, the team spends significant time and effort coaching dozens of development groups on best practices for risk evaluation, secure coding, and vulnerability remediation.

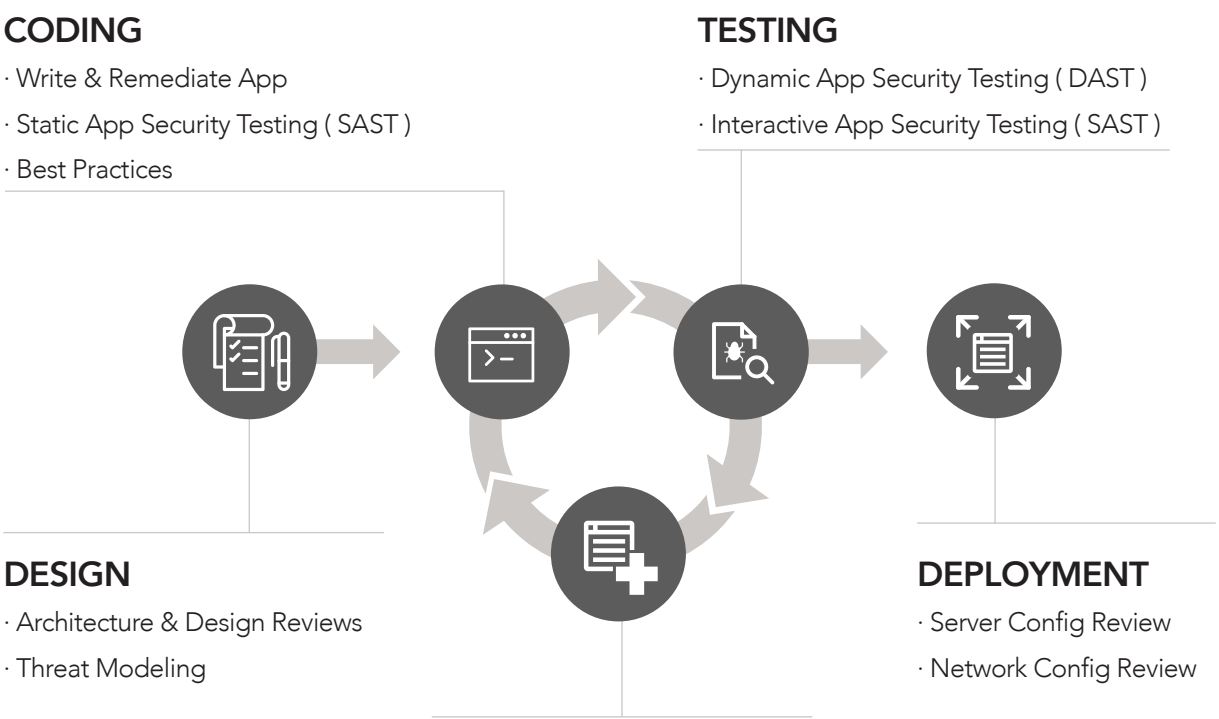
"Our duty is to help developers understand why something will break, not simply that it will. Otherwise you become the white noise that nobody wants to hear. We strive to be enablers, not blockers."

- Fares Alraie, Senior Director - Product Security and Assurance

THE SSDLC: ALWAYS A WORK IN PROGRESS

Four years ago, the company took on the complex yet rewarding task of implementing an organization-wide Secure Software Development Life Cycle (SSDLC) methodology. The team took meticulous steps to create what is now a fully-matured SSDLC model that can support the company's strong product roadmap and expanding business capabilities.

THE SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC)



"Now that our SSDLC model is in a mature state, we're more focused on optimization and introducing new concepts: How can we make the cycle faster? How can it support agile development? How can we better track the effect it has on our ROI? " - Fares Alraie

HOMEGROWN VS. OUTSOURCED SOLUTION?

Applications today are exploitable in many ways, but the most common gateway attacks are still cross-site scripting (XSS), SQL injection (SQLi), and cross-site request forgery (CSRF). The company was using a layered security approach, with various solutions implemented into their SSDLC at different stages. Static code analysis tools helped uncover potential vulnerabilities, but because each finding needed to be assessed and/or remediated, they slowed down the cycle. They also provided zero value for "dead-in-the-water" legacy applications that were outdated or difficult to fix, or for real-time exploits that could only be attempted while an application is running in production.

> "There was room to optimize our SSDLC at the application level. We used this scanner and that filter. We had a WAF enabled, but mostly in listening mode. Our logs could appear clean to penetration testers or network specialists on first glance, but further manual investigation would reveal that attacks were still happening inside the application itself. For example, we'd uncover a persisted cross-site request forgery attempt on a field that was not validating or encoding properly."
>
> - Fares Alraie

Fares Alraie, Senior Director of Product Security and Assurance, together with the rest of the team, sought to create a distributed yet centrally managed model for integrating security features earlier into the application development process. They considered assembling a security team to build programming languages-specific software development kits (SDKs) for its development groups. A management server would hook into each implementation to ensure protection and token/content validation features were consistently being baked into the software. Doing so would help prevent a lot of the attacks and provide the intelligence needed by the company's cybersecurity team.

However, it was debatable whether the project would be a worthwhile use of resources in the long run. The costs to hire a new team, await completion, and keep dozens of SDKs up-to-date would add a significant burden to their already massive security practice.

DETERMINING THE NEED FOR RUNTIME APPLICATION SELF-PROTECTION (RASP)

At around the same time, Prevoty's solution for real-time application threat intelligence and attack prevention were being introduced to the market as a novel approach, featuring SDKs with numerous programming language compatibilities all calling a centralized security engine for analysis and threat neutralization.

Committed to its philosophy that no vendor's solution will be a silver bullet, the company evaluated Prevoty's runtime application self-protection (RASP) offerings with a critical eye:

> "In a large environment like ours, you cannot build or sustain an application security program without a vision, organizational buy-in and a roadmap. Without this strategy, a vendor's tool is simply a stray capability or a series of tasks. If you build a program around your desired capabilities with the proper structure and governance, it becomes easier to plug vendors in the right places to fulfill requirements and optimize the process." - Fares Alraie

It was imperative that Prevoty's service complemented the company's existing, cross-functional SSDLC workflow without causing even the slightest performance hiccup.

> "Prevoty's capabilities fell perfectly into our SSDLC program in two places: its SDKs closed the security loop during our development phases, and its real-time function prevents attacks in our production world." - Fares Alraie

Right away, the company envisioned several use cases for the technology -- the most obvious one being that it would fulfill the need for a centralized, standardized distribution of security technology across its numerous development teams. With Prevoty's approach, for example, developers wouldn't have to manually implement CSRF protection into thousands of individual forms across thousands of applications in the large enterprise's portfolio.

THE VALUE OF NEWFOUND INTELLIGENCE AND ASSURANCE

With Prevoty activated at runtime, the company's applications in production now automatically "phone home" to the security team in real-time with data on where attacks are being found and neutralized. Fares and his team can access these insights inside Prevoty's Management Console or inside a security information and event management (SIEM).

Additionally, the insights help the team make strategic improvements in its secure coding, vulnerability management, and perimeter security configuration practices. As such, the solution is useful not only for detection, but also for process management, education, and real-time prevention.

> "One of our Key Performance Indicators (KPIs) asks, 'How long has it taken us to fix a security finding, from discovery to closure?' The Prevoty SDK reduces the amount of time a developer will need to spend fixing and testing homegrown solutions that don't always withstand every new attack. That cycle of writing, testing, and retesting your own packages will diminish quickly, saving you money." - Fares Alraie

COMPLIANCE

Another important element of ROI is regulatory compliance. The Federal Financial Institutions Examination Council (FFIEC) carefully monitors how this Global Payments Technology Company manages its vulnerabilities. Prevoty plays an active role in compliance by neutralizing the effect of identified vulnerabilities in between extensive re-architecting or code changes and dramatically reducing the possibility that the application's unknown XSS, CSRF, or SQLi vulnerabilities can be exploited.

PERFORMANCE & CUSTOMER SERVICE

Finally, to meet the Global Payment Technology Company's microsecond performance requirements, the engineering team at Prevoty worked closely with the company's security team to ensure seamless integration into the applications and compatibility with their sophisticated Asset Criticality Model -- without any performance degradation.

> "When you're working with a young company, you can give a lot of feedback, and possibly even influence the product strategy. The guys at Prevoty are very open and receptive. Nothing is too far-fetched."
>
> - Fares Alraie

CONCLUSION

Even after seeing a positive effect on long-term viability and ROI, the Global Payments Technology Company continues to find creative ways to expand its use of Prevoty's technology for two objectives: plugging vulnerability holes in existing applications, and building robust security into new applications as part of the SSDLC.

> "Using Prevoty not only makes us feel more at ease, but it actually also makes us feel more precise. It's like finally getting medicine to cure an illness after trying so many other ineffective at-home remedies. Now, our applications talk to us to tell us, 'Look, I got attacked. Here's the field that they used to attack me. Here's what I was able to do to protect myself."
>
> - Fares Alraie

ABOUT PREVOTY

Prevoty has developed a new application security technology that enables applications to be monitored and protected at runtime.

Existing applications can protect themselves against data exfiltration, malicious content, and user identity theft without requiring any changes to the applications themselves.

For new applications, Prevoty's SDKs allow developers to add robust application security capabilities into their applications without requiring any security expertise whatsoever. Prevoty can be delivered as a cloud-based service or as a virtual appliance for on-premise implementations.

Learn more at prevoty.com